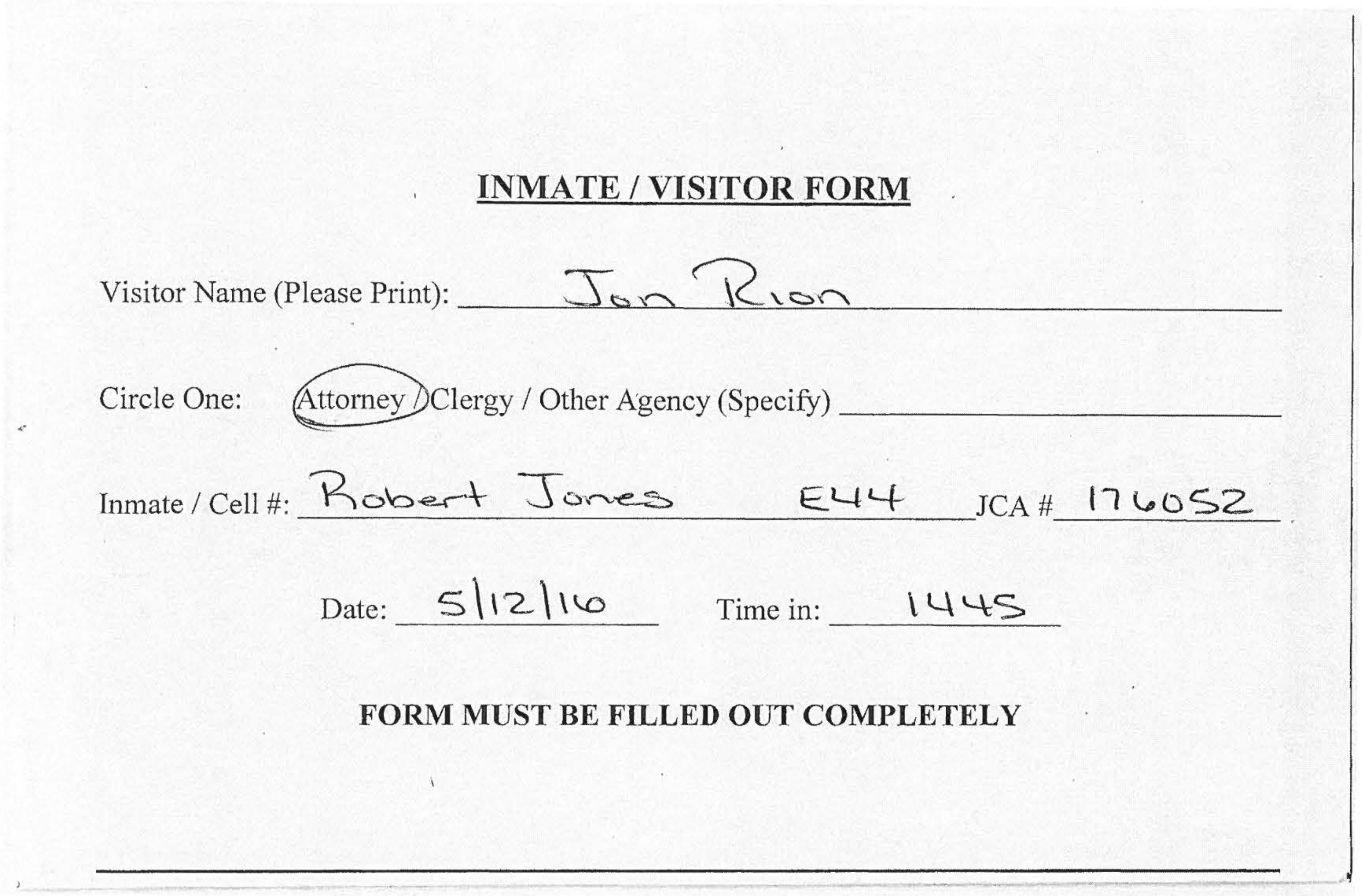
Robert Jones v. United States of America
Cv. Case No. Unassigned
Cr. Case No. 3:16-cr-00026

Exhibit List
for
Motion 28 USC §2255

Exhibit A - Butler County Jail Attorney Visit Form, May 12, 2016
Exhibit B - Letter to counsel asking about status of plea negotiations, etc. June 21, 2016
Exhibit C - Butler County Jail Attorney Visit Form, September 30, 2016
Exhibit D - Butler County Jail Attorney Visit Form, August 23, 2017
Exhibit E - Letter to counsel about mental health history, etc. May 20, 2016
Exhibit F - Butler County Jail Attorney Visit Form, August 29, 2017
Exhibit G - Butler County Jail Attorney Visit Form, September 19, 2017
Exhibit H - Sept. 18, 2013 letter from Mythili Raman to Advisory Committee
Exhibit I - Minutes for 2014 Meeting for Committee on Criminal Rules
Exhibit J - Minutes from March 2015 Meeting of Committee on Criminal Rules
Exhibit K - April 2014 Meeting Agenda for the Committee on Criminal Rules
Exhibit L - Searching & Seizing Training Manual, 2009 - Page 84
Exhibit M - Wikipedia Article on Sandbox (Computer Security)
Exhibit N - Playpen Homepage as it appeared on February 19, 2015
Exhibit O - Google Search results of "list of tor sites"

Exhibit A



INMATE / VISITOR FORM

Visitor Name (Please Print): Jon Rion

Circle One: [✓ Attorney] / Clergy / Other Agency (Specify) ____________

Inmate / Cell #: Robert Jones E44 JCA # 176052

Date: 5/12/16 Time in: 1445

FORM MUST BE FILLED OUT COMPLETELY

Exhibit B

6/21/16

Hey Jon,

It's been a while since I heard from you, so I wanted to check in and see how things are going. Were you able to get the 18? If the government won't go for it I'm still willing to take the 24 unless you think I can get less on the 20-30. We spoke about mitigating factors so let me know what you think.

Did you get a chance to read my last letter about the motion to suppress? I think it's pretty good but we should focus on showing bad faith since the good faith exception is their only out and the FBI clearly would have known the illegality of the warrant. Anyone with even a ba understanding of computer technology would know that remotely searching Tor users would result in global searches, & I, with extremely limited legal experience instantly noticed the issue with the face of the NIT warrant when Stamper showed it to me. Macfarlane swears under penalty of perjury that "on the following person or property (See Attachment A) located in the Eastern District of Virginia, there is now concealed (See Attachment B) evidence of a crime". Attachment A describes the NIT as being deployed "on" the Target Website, obtaining information from the activating computers. How can he swear under penalty of perjury that the information to be seized is located in the EDVA when the entire purpose of the NIT is to discover WHERE a computer is located? Only an idiot would approve this warrant or think there was an ounce of good faith involved. I'd argue that the magistrate wholly abandoned her judicial role by signing this, & bad faith because FBI purposefully misled her.

-Rob Jones

Exhibit C

INMATE / VISITOR FORM

Visitor Name (Please Print): Christian Cavalier

Circle One: [✓ Attorney] / Clergy / Other Agency (Specify) ______

Inmate / Cell #: Robert Jones E28 JCA # 176052

Date: 9-30-16 Time in: 1:04

FORM MUST BE FILLED OUT COMPLETELY

Exhibit D

7

INMATE / VISITOR FORM

Visitor Name (Please Print): Jon Rion

Circle One: Attorney / Clergy / Other Agency (Specify) ____________

Inmate / Cell #: Robert Jones E28 JCA # 176052

Date: 8/23/17 Time in: ____________

FORM MUST BE FILLED OUT COMPLETELY

Exhibit E

Hey JJ, May 20, 2015

You asked me on your last visit to write down my mental health & my abuse history. I'm not 100% sure of the dates so they are mostly estimates.

I suffered sexual & physical abuse from birth until I was 2½ & went to live with foster parents who later adopted me. They said my abuse was linked to Satanic cult activity. I've regularly told therapists that I can't remember any of the abuse, but I actually do remember some things.

Most of my childhood I saw therapists at the Antioch Group in Peoria, IL. I saw Steve Hammond, Janna (last name unknown), & Dr. Singer (I think).
My adoptive Father Steve Jones took me at one point to a child abuse expert in Chicago who examined me & discovered rectal scarring & tissue damage.

Dates	Facilities I Went To -
2003-2005	Piney Ridge Center in Waynesville, MO
2006-2007	Orange Academy in Orange, IL
2003?	Saint Marys Hospital in Decatur, IL
2007?	Methodist Hospital in Peoria, IL

I was treated for ADHD, Bipolar, Psychosis, Anxiety, Borderline Personality Disorder, & Schizophrenia. I've taken Zoloft, Risperdal, Clonodine, Prozac, Liquid Lithium, Depakote, Abilify, Seroquel, & many others (sorry can't spell). If you need me to sign any medical release I will.

- Robert Jones

Exhibit F

2

INMATE / VISITOR FORM

Visitor Name (Please Print): Kion, Jon

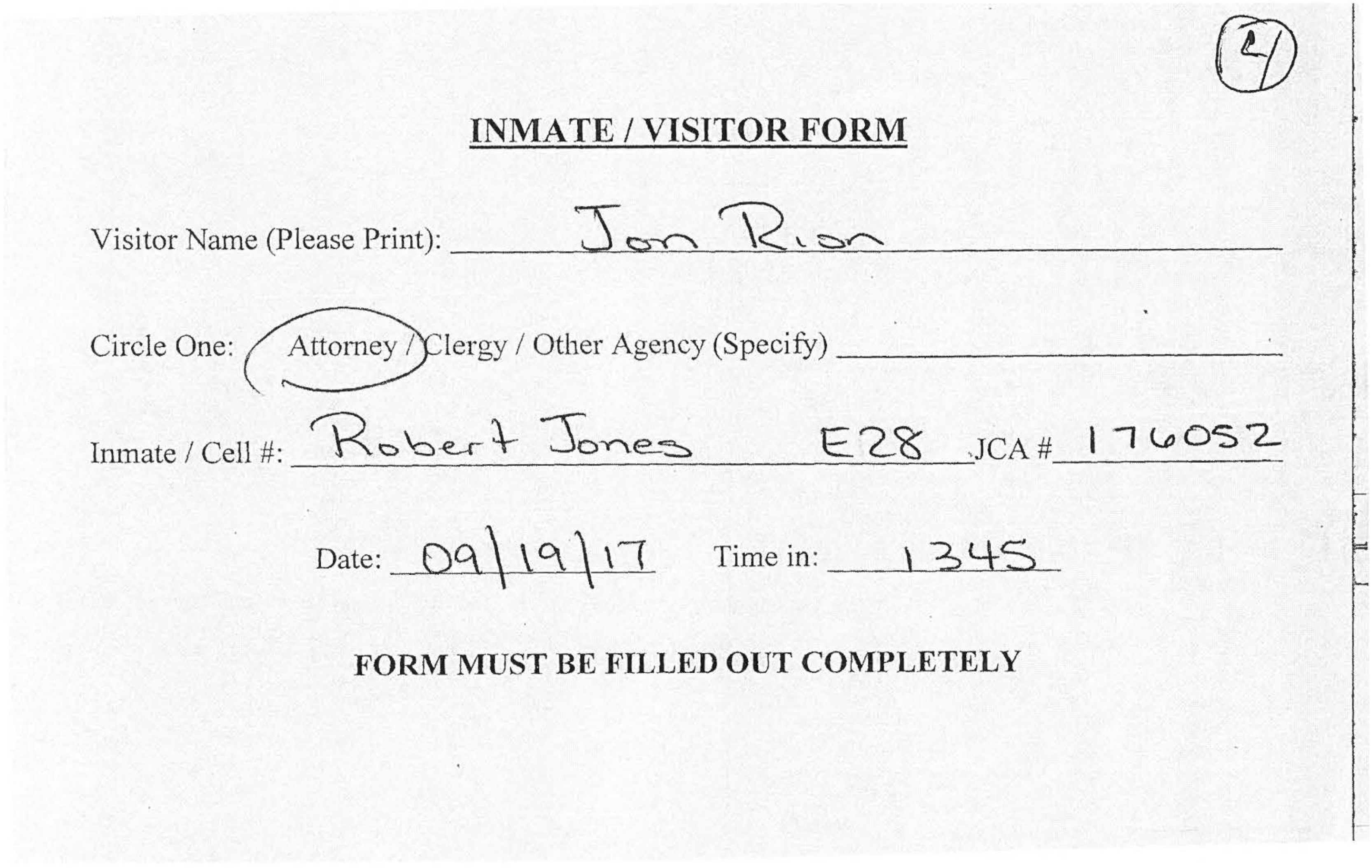
Circle One: [✓ Attorney] / Clergy / Other Agency (Specify)

Inmate / Cell #: Jones, Robert E-2B JCA # 176052

Date: 8-29-17 Time in: 13:22

FORM MUST BE FILLED OUT COMPLETELY

Exhibit G



4

INMATE / VISITOR FORM

Visitor Name (Please Print): Jon Rion

Circle One: [✓ Attorney] / Clergy / Other Agency (Specify) ____________

Inmate / Cell #: Robert Jones E28 JCA # 176052

Date: 09/19/17 Time in: 1345

FORM MUST BE FILLED OUT COMPLETELY

Exhibit H - 1 of 5

U.S. Department of Justice

Criminal Division

13-CR-B

Assistant Attorney General | *Washington, D.C. 20530*

September 18, 2013

The Honorable Reena Raggi
Chair, Advisory Committee on the Criminal Rules
704S United States Courthouse
225 Cadman Plaza East
Brooklyn, NY 11201-1818

Dear Judge Raggi:

The Department of Justice recommends an amendment to Rule 41 of the Federal Rules of Criminal Procedure to update the provisions relating to the territorial limits for searches of electronic storage media. The amendment would establish a court-supervised framework through which law enforcement can successfully investigate and prosecute sophisticated Internet crimes, by authorizing a court in a district where activities related to a crime have occurred to issue a warrant – to be executed via remote access – for electronic storage media and electronically stored information located within or outside that district. The proposed amendment would better enable law enforcement to investigate and prosecute botnets and crimes involving Internet anonymizing technologies, both which pose substantial threats to members of the public.

Background

Rule 41(b) of the Federal Rules of Criminal Procedure authorizes magistrate judges to issue search warrants. In most circumstances, search warrants issue for property that is located within the judge's district. Currently, Rule 41(b) authorizes out-of-district search warrants for: (1) property in the district when the warrant is issued that might be moved outside the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located in a United States territory or a United States diplomatic or consular mission.

Rule 41(b) does not directly address the special circumstances that arise when officers execute search warrants, via remote access, over modern communications networks such as the Internet. Rule 41 should be amended to address two increasingly common situations: (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts.

B

Exhibit H - 2 of 5

The first of these circumstances – where investigators can identify the target computer, but not the district in which it is located – is occurring with greater frequency in recent years. Criminals are increasingly using sophisticated anonymizing technologies when they engage in crime over the Internet. For example, a fraudster exchanging email with an intended victim or a child abuser sharing child pornography over the Internet may use proxy services designed to hide his or her true IP address. Proxy services function as intermediaries for Internet communications: when one communicates through an anonymizing proxy service, the communications pass through the proxy, and the recipient of the communications receives the proxy's IP address, rather than the originator's true IP address. There is a substantial public interest in catching and prosecuting criminals who use anonymizing technologies, but locating them can be impossible for law enforcement absent the ability to conduct a remote search of the criminal's computer. Law enforcement may in some circumstances employ software that enables it through a remote search to determine the true IP address or other identifying information associated with the criminal's computer.

Yet even when investigators can satisfy the Fourth Amendment's threshold for obtaining a warrant for the remote search – by describing the computer to be searched with particularity and demonstrating probable cause to believe that the evidence sought via the remote search will aid in a particular apprehension or conviction for a particular offense – a magistrate judge may decline to issue the requested warrant. For example, in a fraud investigation, one magistrate judge recently ruled that an application for a warrant for a remote search did not satisfy the territorial jurisdiction requirements of Rule 41. *See In re Warrant to Search a Target Computer at Premises Unknown*, ___ F. Supp. 2d ___, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) (noting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology").

Second, criminals are using multiple computers in many districts simultaneously as part of complex criminal schemes, and effective investigation and disruption of these schemes often requires remote access to Internet-connected computers in many different districts. For example, thefts in one district may be facilitated by sophisticated attacks launched from computers in multiple other districts. An increasingly common form of online crime involves the surreptitious infection of multiple computers with malicious software that makes them part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal. Botnets may range in size from hundreds to millions of compromised computers, including home, business, and government systems. Botnets are a significant threat to the public: they are used to conduct large-scale denial of service attacks, steal personal and financial data, and distribute malware designed to invade the privacy of users of the host computers.

Effective investigations of these sophisticated crimes often require law enforcement to act in many judicial districts simultaneously. Under the current Rule 41, however, except in cases of domestic or international terrorism, investigators may need to coordinate with agents,

Exhibit H - 3 of 5

prosecutors, and magistrate judges in every judicial district in which the computers are known to be located to obtain warrants authorizing the remote access of those computers. For example, a large botnet investigation is likely to require action in all 94 districts, but coordinating 94 simultaneous warrants in the 94 districts would be impossible as a practical matter. At a minimum, requiring so many magistrate judges to review virtually identical probable cause affidavits wastes judicial and investigative resources and creates delays that may have adverse consequences for the investigation. Authorizing a court in a district where activities related to a crime have occurred to issue a warrant for electronic storage media within or outside the district would better align Rule 41 with the extent of constitutionally permissible warrants and remove an unnecessary obstruction currently impairing the ability of law enforcement to investigate botnets and other multi-district Internet crimes.

Thus, while the Fourth Amendment permits warrants to issue for remote access to electronic storage media or electronically stored information, Rule 41's language does not anticipate those types of warrants in all cases. Amendment is necessary to clarify the procedural rules that the government should follow when it wishes to apply for these types of warrant.

Language of Proposed Amendment

Our proposed amendment includes two parts. First, we propose adding the following language at the end of subsection (b):

> and (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant, to be executed via remote access, for electronic storage media or electronically stored information located within or outside that district.

Second, we propose adding the following language at the end of subsection (f)(1)(C):

> In a case involving a warrant for remote access to electronic storage media or electronically stored information, the officer executing the warrant must make reasonable efforts to serve a copy of the warrant on an owner or operator of the storage media. Service may be accomplished by any means, including electronic means, reasonably calculated to reach the owner or operator of the storage media. Upon request of the government, the magistrate judge may delay notice as provided in Rule 41(f)(3).

Exhibit H - 4 of 5

Discussion of Proposed Amendment

The proposed amendment authorizes a court with jurisdiction over the offense being investigated to issue a warrant to remotely search a computer if activities related to the crime under investigation have occurred in the court's district. In other circumstances, the Rules or federal law recognize that it can be appropriate to give magistrate judges nationwide authority to issue search warrants. For example, in terrorism investigations, the current Rule 41(b)(3) allows a magistrate judge "in any district in which activities related to the terrorism may have occurred" to issue a warrant "for a person or property within or outside that district." This approach is also similar to the current rule for a warrant requiring communication service providers to disclose electronic communications: a court with "jurisdiction over the offense being investigated" can issue such a warrant. *See* 18 U.S.C. §§ 2703(a) & 2711(3)(A)(I); *United States v. Bansal,* 663 F.3d 634, 662 (3d Cir. 2011); *United States v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008). Mobile tracking device warrants may authorize the use of tracking devices outside the jurisdiction of the court, so long as the device was installed in that jurisdiction. Fed. R. Crim. P. 41(b)(4); 18 U.S.C. § 3117(a). In the proposed amendment, the phrase "any district where activities related to a crime may have occurred" is the same as the language setting out the jurisdictional scope of Rule 41(b)(3).

The amendment provides that notice of the warrant may be accomplished by any means reasonably calculated to reach an owner or operator of the computer or – as stated in the amendment, which uses existing Rule 41 language – the "storage media or electronically stored information." In many cases, notice is likely to be accomplished electronically; law enforcement may not have a computer owner's name and street address to provide notice through traditional mechanisms. The amendment also requires that the executing officer make reasonable efforts to provide notice. This standard recognizes that in unusual cases, such as where the officer cannot reasonably determine the identity or whereabouts of the owner of the storage media, the officer may be unable to provide notice of the warrant. *Cf.* 18 U.S.C. § 3771(c)(1) (officers "shall make their best efforts to see that the crime victims are notified of ... the rights described in subsection (a)").

In light of the presumption against international extraterritorial application, and consistent with the existing language of Rule 41(b)(3), this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries. The Fourth Amendment does not apply to searches of the property of non-United States persons outside the United States, *see United States v. Verdugo-Urquidez*, 494 U.S. 259, 261 (1990), and the Fourth Amendment's warrant requirement does not apply to searches of United States persons outside the United States. *See United States v. Stokes*, ___ F.3d ___, 2013 WL 3948949 at *8-*9 (7th Cir. Aug. 1, 2013); *In re Terrorist Bombings*, 552 F.3d 157, 170-71 (2d Cir. 2008). Instead, extraterritorial searches of United States persons are subject to the Fourth Amendment's "basic requirement of reasonableness." *Stokes*, 2013 WL 3948949 at

Exhibit H - 5 of 5

*9; *see also In re Terrorist Bombings*, 552 F.3d at 170 n.7. Under this proposed amendment, law enforcement could seek a warrant either where the electronic media to be searched are within the United States or where the location of the electronic media is unknown. In the latter case, should the media searched prove to be outside the United States, the warrant would have no extraterritorial effect, but the existence of the warrant would support the reasonableness of the search.

* * *

We believe that timely and thorough consideration of this proposed amendment by the Advisory Committee is appropriate. We therefore ask that the Committee act at its November meeting to establish a subcommittee to examine this important issue. Criminals are increasingly using sophisticated technologies that pose technical challenges to law enforcement, and remote searches of computers are often essential to the successful investigation of botnets and crimes involving Internet anonymizing technologies. Moreover, this proposal would ensure a court-supervised framework through which law enforcement could successfully investigate and prosecute such crimes.

We look forward to discussing this with you and the Committee.

Sincerely,

Mythili Raman

Mythili Raman
Acting Assistant Attorney General

cc: Professor Sara Sun Beale, Reporter
Professor Nancy J. King, Reporter

Exhibit 1 - 1 of 3

the agenda book. The proposal would amend the Rule 41 to add new subdivision (b)(6):

> A magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district.

This amendment would authorize a magistrate to issue a warrant to search allowing officers to remotely search and seize information on a computer, even if that computer is located outside the magistrate's district, so long as criminal activity has occurred within that district. Rule 41 generally limits warrants to searches and seizures within the district, but it already provides authority for a judge to issue a warrant for a search or seizure outside the district in four other situations, including the use of tracking devices. The amendment seeks only to refine the territorial limits; it does not alter the constitutional constraints, such as the particularity requirement. Any constitutional restriction should be addressed by each magistrate with each warrant request.

As to the notice requirement, Judge Keenan continued, the proposed amendment reads:

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of it on the person whose property was searched or whose information was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

This amendment would clarify that officers must make reasonable efforts to provide notification of the search or seizure.

Judge Keenan reported that the Subcommittee held four telephone conferences and considered several memoranda, which are included in the agenda book. The materials also include sample warrants. In the fourth conference call, the Subcommittee approved the version of the proposed amendment that was identical to the version before the Committee, except for a few style changes. Judge Keenan noted that Judge Kethledge, who could not be at this meeting, served as a member of the Subcommittee, had indicated approval of the proposal, and that one member dissented from the Subcommittee's proposed amendment. Finally, he recognized that some Committee members may not have had time to read and analyze the memorandum from the American Civil Liberties Union.

Exhibit I - 2 of 3

Judge Raggi asked the Department of Justice to speak to the proposal.

Assistant Attorney General O'Neil said the proposal is meant to address three scenarios. The first is to provide authority for a magistrate to issue a warrant to search with remote access for the location of a computer whose location is unknown, possibly in another district. The second is to provide authority for a judge to issue a warrant to search multiple computers in known locations outside the district. The third is to provide authority for a judge to issue a warrant to conduct a remote access search in a district outside the district where the warrant is being sought, as an ancillary request to a physical search request.

Assistant Attorney General O'Neil emphasized that the proposal does not provide authority for the government to conduct any new kind of search or to use any new tools. It does not change anything about the substantive standards that the government must satisfy in order to obtain a warrant or address the substantive requirements of particularity or probable cause. All it does, he explained, is address the venue question–the question of which judge can issue a warrant that, as the law develops, the Fourth Amendment allows.

Assistant Attorney General O'Neil spoke to two concerns raised by the proposal. As to forum or judge shopping, he said that the same concern was raised by the Electronic Communications Privacy Act (ECPA), which already allows a judge in one district to issue a warrant in another district. Congress nevertheless approved this scheme, and the Department was not aware of any complaints about this problem under the ECPA. The second concern he noted was that the proposal could be used to circumvent ECPA or as an alternative means that is less protective than ECPA. The Department did not think that was a problem. The same standards of particularity and probable cause apply to both ECPA and warrants under the proposed Rule 41 remote access searches. Also, prosecutors can already obtain warrants for remote access searches under the present rule. The only question is whether the judge who is most familiar with the facts of an investigation can issue a warrant for information stored outside that judge's district.

Mr. Wroblewski stated that when investigators don't know where the computer is, it is very important to be able to learn that information. He recognized that the ACLU has argued that there ought to be oversight of the code that the government uses to do this, that there ought to be more transparency, and that the code has potential to do harm. The Department recognizes those concerns, he explained, but this Committee is not the place to address them. Some of the issues are Constitutional and will be addressed by magistrate judges one warrant at a time. Some of them will ultimately be addressed by Congress in determining what is and is not permissible. What this proposal tries to address are the three practical realities summarized earlier and in the memos included in the materials.

Exhibit I - 3 of 3

Judge Raggi reminded members that if the Committee were to approve a proposed amendment at the meeting, even if everything goes smoothly, it will be a three-year process. She suggested taking the package apart to attempt to identify where there was agreement and where there wasn't.

Turning to the situation in which the government doesn't know where the computer is, she said that declining to modify the rule leaves the government without a way to get a warrant. One issue is whether the rules should require the government to make a showing that they don't know where the computer is. One member suggested that the proposal require such a showing, while the government sees this as an undue burden.

Judge Raggi asked the Department to comment its opposition to a preliminary showing. Mr. Wroblewski indicated that the Department is concerned that depending upon how it is crafted this requirement could lead to litigation over how much the government knew or could learn, but he noted that it might be possible to draft language that referred to the type of technology.

Judge Raggi asked for an explanation of the rationale for requiring a preliminary showing. A member said that adding language that "the location cannot reasonably be ascertained" would respond to Magistrate Smith's opinion, and would operate like other judicial assessments that a judge makes in the warrant process, none of which form the basis for later litigation. It is not a constitutional argument so there could be no basis for suppression, nor is suppression a remedy for violation of the rule.

Another member pointed out that there are limited resources the government can use to track down the location of a computer that had been disguised by anonymizing software. If there is a showing required, it should be clear that the NSA and CIA need not get involved. The entire federal government shouldn't have to gear up to prove this for each warrant.

Mr. Wroblewski commented that language that does not turn on the government's knowledge but rather on the type of technology used would avoid these concerns. Assistant Attorney General O'Neil suggested that something like "an investigation involving the use of technological means to conceal identity" might work.

A member asked those supporting a preliminary showing why this would be unlike Title III, where the failure to comply with procedural requirements forms the basis for defense litigation. A member favoring a preliminary showing responded that this assessment would be the same as other judicial assessments under the current rule concerning the property's location, which are not currently litigated because suppression is not a remedy for violations of the rule.

Exhibit J - 1 of 2

government's view we should apply the same rules, as much possible, to technology as to the physical world: the same probable cause rules, the same particularity rules, and as much as possible the same procedural rules. Remote searches are conducted today, and by themselves do not present new issues. What is new is the ease with which someone can conceal his location by anonymizing technology, and the amendment addresses the venue gap created by that reality. The proposed amendment is privacy enhancing, because it provides a venue in which the government can seek advance judicial authorization of a search, just as it would before conducting a search of someone's home. This process allows the courts to apply the basic principles of the Fourth Amendment to new forms of technology, as they have done, for example, with heat sensors and tracking devices. The government's goal here is to secure a warrant, a privacy enhancing process.

Although several commenters argued that the Committee should follow the precedent of Title III and wait for Congress to act, Professor Beale observed that the history of Title III cuts the other way. Title III was enacted *after* the case law on wiretaps developed, just as the case law is doing now with other forms of technology in cases such as *Riley v. California*. In general, Congress has legislated after a sufficient number of cases have been litigated to shed light on the policy issues. In the case of new technology, the courts are grappling with questions of what information is protected by the Fourth Amendment as well as how requirements such as particularity apply in new contexts. The proposed venue provision would permit the same process to operate with remote electronic searches, allowing the courts to rule on the issues of concern to the commenters. Although it is possible that providing venue will increase the number of remote searches, Professor Beale noted that it may instead increase the number of remote searches reviewed by the courts ex ante in the warrant application process, rather than only ex post following a search yielding information that the government seeks to introduce at trial.

Judge Sutton complimented the Committee on narrowing the proposed amendment and being responsive to the public concerns. He observed that approving venue for warrant applications is not the same as approving remote electronic searches. Rather, it permits more litigation as to search warrants that will shed light on the process and issues. He emphasized that the Rules Enabling Act tells the judiciary to promulgate rules of procedure, not to wait for Congress to act first. Instead, Congress responds to proposed rules.

The member who had stated opposition to the proposed amendment acknowledged that courts must deal with the issues raised by new technology but remained unable to support the amendment, characterizing it as substantive and reiterating there are many unknowns.

Discussion turned to the question what would be known or unknown in the warrant applications covered by the amendment. Mr. Bitkower noted that to obtain any warrant the government must know what crime it is investigating and what it is looking for. In the anonymizing software cases covered by the amendment, the only new unknown is the physical location of the device to be searched. Because Rule 41 currently provides no venue for a warrant application in such cases, if the government deems a situation serious but not "exigent," it must

Exhibit J - 2 of 2

now either wait or pursue other investigative techniques that may in some cases be more invasive. In botnet cases, he noted, the problem is the large number of computers, not the lack of information.

A member expressed the view that the most significant unknowns would arise in the botnet cases: what information might be sought from thousands or even millions of computers that had been hacked. Moreover, the technology required for different botnets may vary. He also noted that the Committee was being forward thinking in addressing these issues, since there have been relatively few botnet investigations and only one decision holding that a court cannot issue a warrant when anonymizing software has disguised the location of the device to be searched. It was sensible, he concluded, to address both problems with a narrowly tailored "surgical" amendment.

Agreeing that each criminal botnet is unique, Mr. Bitkower explained that one function of warrants under the proposed amendment could be to map a botnet before seeking to shut it down, collecting the IP addresses of the affected computers to determine the botnet's size and where the computers are located. In previous botnet investigations, the cumbersome requirement of seeking a warrant in each district played a role in determining the government's strategy, and civil injunctions were used. He also noted that warrant applications under the amendment would vary widely: in some cases they may be quite simple and narrow (as in the case of a single email account when the government has already obtained the password), but in other cases there will be more significant complications and new issues on which courts will have to rule.

Members compared the procedural options under the current rule and the proposed amendment in the investigation of the hacking of a major corporation or institution such as the New York Stock Exchange. If the NYSE were hacked and anonymizing software disguised the location of a device the government had probable cause to search, members speculated that the government would conduct a search under some legal theory. They identified three possible scenarios under the current rule: (1) the government might persuade a court in the Southern District of New York to grant the warrant, and then claim good faith reliance if the warrant were later invalidated for lack of venue; (2) a court in the Southern District might find probable cause but determine it had no authority to issue a warrant, in which case the government might conduct a warrantless search and argue that the failure to obtain a warrant was harmless error because the search was nevertheless supported by probable cause; or (3) the government might search without a warrant under a claim of exigent circumstances. Members expressed the view that these examples showed why it would be preferable to amend Rule 41 to provide venue for warrant applications, so that courts asked to approve such warrants would be able to focus on the constitutional issues presented by remote computer searches. Concerns about the judiciary's understanding of the technology could be addressed by judicial education.

In response to the question how frequently the government expects to seek warrants under the proposed amendment, Mr. Bitkower noted the use of anonymizing technology by criminals is likely to become much more common. Until recently only sophisticated criminals employed

Exhibit K - 1 of 3

process and the desirability of a comprehensive approach, rather than one that would make a series of amendments to the same rule. Members noted, however, that they expected to learn more from public comments by various stakeholders if the proposal is approved for publication.

This memorandum first describes the proposed amendment and the justifications for it, and then reviews the issues and concerns discussed by the Subcommittee.

The proposal has two parts. The first change is an amendment to Rule 41(b), which generally limits warrant authority to searches within a district,[2] but permits out-of-district searches in specified circumstances.[3] The amendment would add remote access searches for electronic information to the list of other extraterritorial searches permitted under Rule 41(b). Language in a new subsection 41(b)(6) would authorize a court to issue a warrant to use remote access to search electronic storage media and seize electronically stored information inside *or outside* of the district.

The second part of the proposal is a change to Rule 41(f)(1)(C), regulating notice that a search has been conducted. New language would be added at the end of that provision indicating the process for providing notice of a remote access search.

A. **Reasons for the proposal.**

Rule 41's territorial limitation, limiting searches to locations within a district, creates special difficulties for the Government when investigating crimes involving electronic information. The proposal speaks to three different scenarios impacted by the territorial restriction, each involving remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet.

Scenario 1. The proposal would enable investigators to obtain a warrant to search with remote access computers with unknown locations. This situation might arise where a particular computer is likely to contain evidence of crime--a person is using the computer to send pornography by email, for example--but the person using that computer is using anonymizing tools that disguise the computer's true IP address so that agents are unable to identify its location. A warrant for a remote access search would enable investigators to send an email, remotely install software on the device receiving the email, and determine the true IP address or identifying information for that device. Several examples of an affidavit seeking a warrant to conduct such a search are attached, under Tab D. Some judges have reportedly approved such searches,[4] but one judge recently concluded that the territorial requirement in Rule 41 precluded

[2] Rule 41(b)(1) ("a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district").

[3] Currently, Rule 41(b) (2) – (5) authorize out-of-district or extra-territorial warrants for: (1) property in the district when the warrant is issued that might be moved outside the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located in a United States territory or a United States diplomatic or consular mission.

[4] In addition to the examples provided by the Department, a critical assessment noting additional examples appears in Craig Timberg and Ellen Nakashima, "FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware

a warrant for a remote search when the location of the computer was not known, suggesting that the Committee should consider updating the territorial limitation to accommodate advancements in technology. See Tab C, DOJ Letter 9/18/2013, at 2 (citing *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (noting that "there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology")); Tab H, DOJ Memo 3/5/2014.

Scenario 2. The proposal would enable investigators to obtain warrants to search computers in many districts simultaneously. It is not unusual for on-line criminal activity to involve multiple computers in several districts. One example is the "botnet"--a collection of computers in several (potentially all) districts, under the remote command and control of a criminal who infects those computers with malicious software so that he may use them to interrupt service, steal data, or distribute more malware. "Under the current Rule 41," the Department argued, "except in cases of domestic or international terrorism, investigators may need to coordinate with agents, prosecutors, and magistrate judges in every judicial district in which the computers are known to be located to obtain warrants authorizing the remote access of those computers." Tab C, DOJ Letter 9/18/2013, at 2-3. Under the proposed amendment, a warrant for a remote search in this situation would enable investigators to remotely install software on a large number of affected computers all at once. When the locations of those computers are known to be in more than one district, this authorization would eliminate the burden of attempting to secure separate warrants in numerous districts. If the locations of the various computers are *not* known, the proposal would permit the government to remotely access multiple devices to obtain identifying information. See, under Tab D, Sample Botnet Affidavit.

Scenario 3. The proposal would permit a judge to authorize a search for electronic information accessible from a computer at a known location when the information is stored remotely in another district. The Department provided this example:

> [S]uppose that officers execute a warrant to search a business located in San Francisco and that, upon entry, they discover that the business stores its documents with a cloud-based server. Under the current version of Rule (assuming the requisite probable cause and particularity requirements are met), a magistrate in the Northern District of California could issue a warrant authorizing agents to search the business and, while they are present at the business, access any cloud-based storage located within the district (such as a DropBox account).

The amendment "would clarify that the magistrate could equally authorize the agents to access such storage in *any* district, including an unknown district." Tab H, DOJ memo 3/5/2014, at 3 (emphasis added). The Department argued that without the authorization in the proposed

for surveillance." Wash. Post., Dec 6, 2013, *available at* http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html

Exhibit K - 3 of 3

On the substance of Professor Kerr's concerns -- Professor Kerr's chief concern surrounds the constitutional requirements for warrants for searches of electronic information. For example, Professor Kerr is concerned with searches of multiple computers through a single warrant. We recognize that this is an important issue and may be litigated in an appropriate case. But as we discussed before in exploring some members' concerns over the particularity requirement for warrants for electronic information, the proposed amendment cannot and does not address substantive constitutional questions. The language of our proposed rule does not address the question of multiple searches using a single warrant. And as requested, we have drafted Committee Note language with the Committee reporters to ease the concerns that the amendment might be read as an attempt to influence resolution of this or other constitutional issues.

On the other hand, we are indeed seeking a rule that would authorize a federal judge to issue a warrant for a remote search of electronic media located in a known – or unknown – location outside her district where the crime occurred in the district, including for those cases when a search would require coordination of simultaneous action in many districts at once. Despite Professor Kerr's concerns, we think this is the right policy and the right rule for several reasons.

First, Congress and the federal courts have already recognized that because of the very nature of electronic information, multijurisdictional judicial authorization for obtaining such information is good public policy. In the context of pen registers, wiretaps and the Electronic Communications Privacy Act, multijurisdictional authorization for obtaining electronic information is already the law.

For example, Professor Kerr notes in his memorandum that the proposed amendment could be used to obtain warrants in multi-district cases that do not involve botnets, such as where a suspect uses a Dropbox account to store information. He is correct. In such cases, however, Congress has already authorized a judge in the district where the crime occurred – rather than in the district where the data is stored – to issue an order for law enforcement to obtain the information. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A) and 2711(3)(A) (authorizing a court with "jurisdiction over the offense being investigated" to issue an order requiring an online service provider to disclose information it stores regarding a customer). These existing multijurisdictional authorizations have raised no serious concerns and our proposal is consistent with them.

Second, as we have previously indicated, investigations that require obtaining warrants in multiple districts for searches of computers involved in a single crime create serious practical obstacles for law enforcement while also wasting judicial resources. Rule 41 already recognizes these realities in terrorism cases and provides for multijurisdictional reach in those cases.

Third, providing multijurisdictional reach for searches of electronic media will facilitate a more robust review of the warrant applications. It will permit a single judge with knowledge of the investigation – in the district where the investigation is taking place – to review all warrant

Exhibit L

6. Multiple Warrants in Network Searches

☞ Agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations.

Fed. R. Crim. P. 41(a) states that a magistrate judge located in one judicial district may issue a search warrant for "a search of property . . . within the district," or "a search of property . . . outside the district if the property . . . is within the district when the warrant is sought but might move outside the district before the warrant is executed." Rule 41 defines "property" to include "information," *see* Fed. R. Crim. P. 41(a)(2)(A), and the Supreme Court has held that "property" as described in Rule 41 includes intangible property such as computer data. *See United States v. New York Tel. Co.*, 434 U.S. 159, 170 (1977). Although the courts have not directly addressed the matter, the language of Rule 41 combined with the Supreme Court's interpretation of "property" may limit searches of computer data to data that resides in the district in which the warrant was issued. *Cf. United States v. Walters*, 558 F. Supp. 726, 730 (D. Md. 1980) (suggesting such a limit in a case involving telephone records).

A territorial limit on searches of computer data poses problems for law enforcement because computer data stored in a computer network can be located anywhere in the world. For example, agents searching an office in Manhattan pursuant to a warrant from the Southern District of New York may sit down at a terminal and access information stored remotely on a computer located in New Jersey, California, or even a foreign country. A single file described by the warrant could be located anywhere on the planet, or could be divided up into several locations in different districts or countries. Even worse, it may be impossible for agents to know when they execute their search whether the data they are seizing has been stored within the district or outside of the district. Agents may in some cases be able to learn where the data is located before the search, but in others they will be unable to know the storage site of the data until after the search has been completed.

When agents can learn prior to the search that some or all of the data described by the warrant is stored in a different location than where the agents will execute the search, the best course of action depends upon where the remotely stored data is located. When the data is stored remotely in two or more different places within the United States and its territories, agents should obtain additional warrants for each location where the data resides to ensure

Exhibit M - 1 of 2

WIKIPEDIA

Sandbox (computer security)

In computer security, a **sandbox** is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system.[1] A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as storage and memory scratch space. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization. Sandboxing is frequently used to test unverified programs that may contain a virus or other malicious code, without allowing the software to harm the host device.[2]

Contents

Implementations

A sandbox is implemented by executing the software in a restricted operating system environment, thus controlling the resources (for example, file descriptors, memory, file system space, etc.) that a process may use.[3]

Examples of sandbox implementations include the following:

- Linux application sandboxing, built on Seccomp, cgroups and Linux namespaces. Notably used by Systemd, Google Chrome, Firefox, firejail.
- Google Sandboxed API[4]
- A jail: network-access restrictions, and a restricted file system namespace. Jails are most commonly used in virtual hosting.[5]
- Rule-based execution gives users full control over what processes are started, spawned (by other applications), or allowed to inject code into other applications and have access to the net, by having the system assign access levels for users or programs according to a set of determined rules.[6] It also can control file/registry security (what programs can read and write to the file system/registry). In such an environment, viruses and Trojans have fewer opportunities of infecting a computer. The SELinux and Apparmor security frameworks are two such implementations for Linux.
- Virtual machines emulate a complete host computer, on which a conventional operating system may boot and run as on actual hardware. The guest operating system runs sandboxed in the sense that it does not function negatively on the host and can only access host resources through the emulator.

- Sandboxing on native hosts: Security researchers rely heavily on sandboxing technologies to analyse malware behavior. By creating an environment that mimics or replicates the targeted desktops, researchers can evaluate how malware infects and compromises a target host. Numerous malware analysis services are based on the sandboxing technology.[7]
- Native Client is a sandbox for running compiled C and C++ code in the browser efficiently and securely, independent of the user's operating system.[8]
- Capability systems can be thought of as a fine-grained sandboxing mechanism, in which programs are given opaque tokens when spawned and have the ability to do specific things based on what tokens they hold. Capability-based implementations can work at various levels, from kernel to user-space. An example of capability-based user-level sandboxing involves HTML rendering in a Web browser.
- Secure Computing Mode (seccomp) is a sandbox built in the Linux kernel. When activated in strict mode, seccomp only allows the `write()`, `read()`, `exit()`, and `sigreturn()` system calls.
- HTML5 has a "sandbox" attribute for use with iframes.[9]
- Java virtual machines include a sandbox to restrict the actions of untrusted code, such as a Java applet.
- The .NET Common Language Runtime provides Code Access Security to enforce restrictions on untrusted code.
- Software Fault Isolation (SFI),[10] allows running untrusted native code by sandboxing all store, read and jump assembly instructions to isolated segments of memory.
- Windows Vista and later editions include a "low" mode process running, known as "User Account Control" (UAC), which only allows writing in a specific directory and registry keys. Windows 10, from version 1903 (released May 2019), provides a feature known as "Windows Sandbox: an isolated, temporary, desktop environment where you can run untrusted software without the fear of lasting impact to your PC". [11]

Some of the use cases for sandboxes include the following:

- Online judge systems to test programs in programming contests.
- New-generation pastebins allowing users to execute pasted code snippets on the pastebin's server.

See also

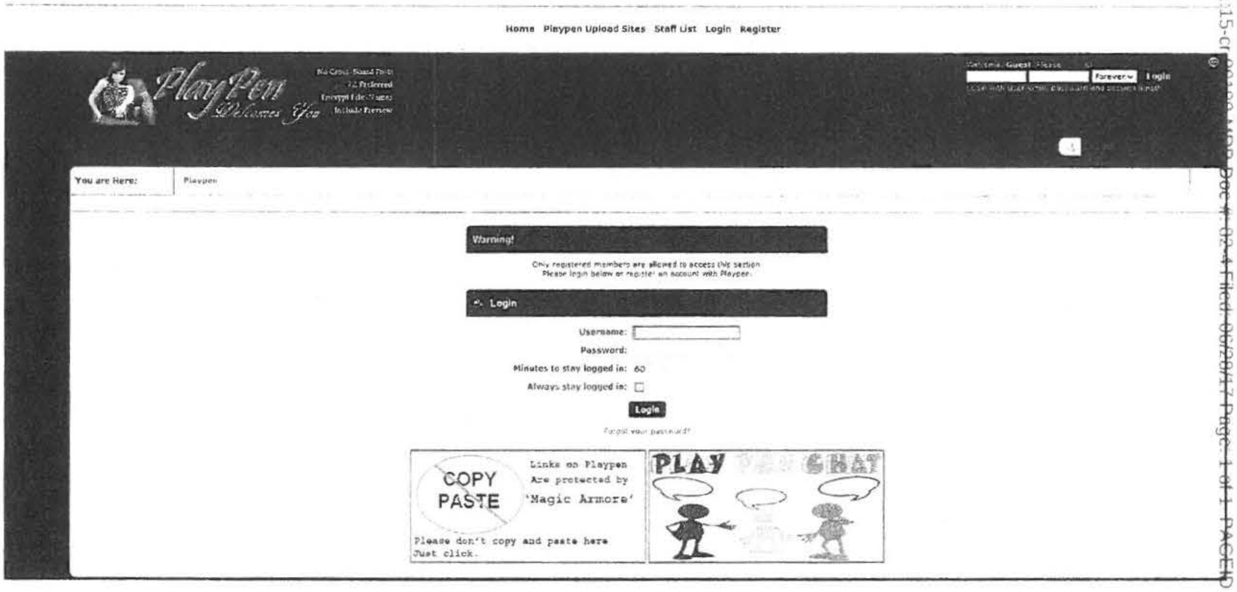
- Sandboxie
- seccomp
- Shade sandbox
- Tor (anonymity network)
- Solebit

References

1. Ian Goldberg; David Wagner; Randi Thomas & Eric Brewer (1996). "A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker)" (http://www.usenix.org/publications/library/proceedings/sec96/full_papers/goldberg/goldberg.pdf) (PDF). *Proceedings of the Sixth USENIX UNIX Security Symposium*. Retrieved 25 October 2011.
2. Geier, Eric (2012-01-16). "How to Keep Your PC Safe With Sandboxing" (http://www.techhive.com/article/247416/how_to_keep_your_pc_safe_with_sandboxing.html). TechHive. Retrieved 2014-07-03.

Exhibit N

Case: 1:15-cr-00106-MDR Doc #: 62-4 Filed: 06/20/17 Page: 1 of 1 PAGEID #: 559



Home Playpen Upload Sites Staff List Login Register

Welcome, Guest. Please

Forever

Login

You are Here: Playpen

Warning!

Only registered members are allowed to access this section
Please login below or register an account with Playpen.

Login

Username:

Password:

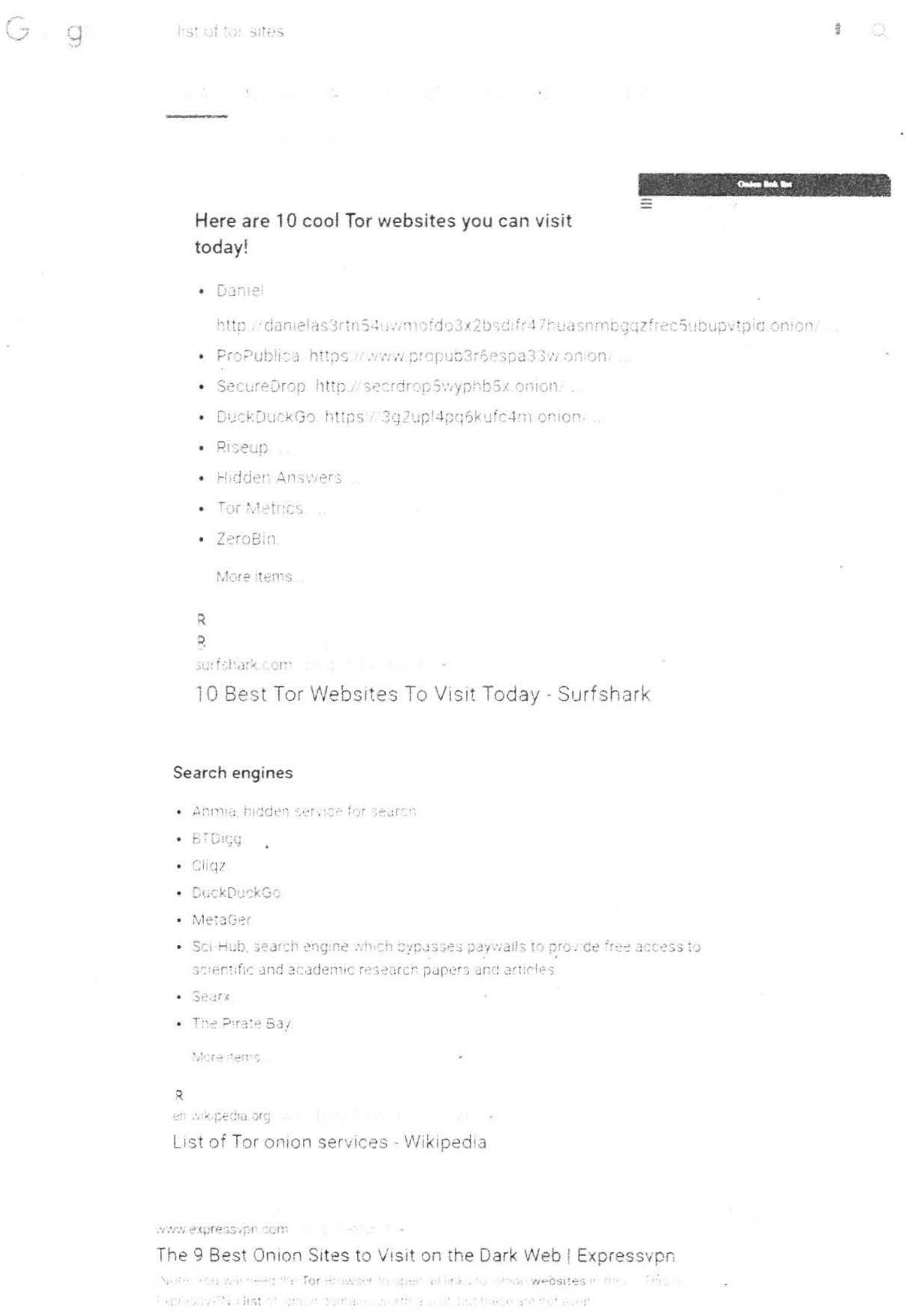
Minutes to stay logged in: 60

Always stay logged in: □

Login

Forgot your password?

Exhibit O - 1 of 2



Here are 10 cool Tor websites you can visit today!

- Daniel http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion/ ...
- ProPublica. https://www.propub3r6espa33w.onion/ ...
- SecureDrop. http://secrdrop5wyphb5x.onion/ ...
- DuckDuckGo. https://3g2upl4pq6kufc4m.onion/ ...
- Riseup. ...
- Hidden Answers. ...
- Tor Metrics. ...
- ZeroBin.

More items...

R
R
surfshark.com

10 Best Tor Websites To Visit Today - Surfshark

Search engines

- Ahmia, hidden service for search
- BTDigg
- Cliqz
- DuckDuckGo
- MetaGer
- Sci-Hub, search engine which bypasses paywalls to provide free access to scientific and academic research papers and articles
- Searx
- The Pirate Bay

More items...

R
en.wikipedia.org

List of Tor onion services - Wikipedia

www.expressvpn.com

The 9 Best Onion Sites to Visit on the Dark Web | Expressvpn

Note: You will need the Tor Browser to open all links to other websites in this ... This is ExpressVPN's list of onion domains worth a visit, but these are not even

Exhibit O - 2 of 2

vpnoverview.com

10 websites on the Dark Web worth visiting | VPNOverview

[illegible]

Hidden Wiki · Not Evil · BBC Tor Mirror · Tor Metrics

thehiddenwiki.org

Hidden Wiki | Tor .onion urls directories

[illegible]

People also ask

[illegible]

[illegible]

Can you browse normal sites on Tor?

[illegible]

The best websites of the Tor Deep Web Network | Web Design ...

[illegible]

www.makeuseof.com

The Best Dark Web Websites You Won't Find on Google ...

TorLinks [illegible] TorLinks [illegible] sites [illegible]

www.makeuseof.com

How to Find Active .Onion Dark Web Sites (And Why You ...

[illegible] sites [illegible] sites [illegible]

[illegible]

15 Best Dark Web Websites You Should Explore - PureVPN ...

[illegible] websites [illegible]

www.vpnmentor.com

What are the Best .onion Sites & How to Access Them Safely ...

[illegible] sites [illegible] websites [illegible] Tor [illegible] list?

G [illegible] g [illegible] >

1 2 3 4 5 6 7 8 9 10 Next